UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/662,996	09/15/2003	Takashi Kawasaki	0828.68359	2241

24978 7590 06/26/2007
GREER, BURNS & CRAIN
300 S WACKER DR
25TH FLOOR
CHICAGO, IL 60606

EXAMINER	
LUDWIG, PETER L	
ART UNIT	**PAPER NUMBER**
3621	

MAIL DATE	DELIVERY MODE
06/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/662,996	**Applicant(s)** KAWASAKI ET AL.	
	Examiner Peter L. Ludwig	**Art Unit** 3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/13/2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *6-14,16,18 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *6-14,16,18 and 20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Acknowledgements

1. This Office Action has been given Paper No. 20070613 for reference purposes only.

2. This Office Action is in correspondence to Amendment A filed on 04/13/2007.

3. Claims 1-5, 15, 17, and 19 have been cancelled.

4. Claims 6-14, 16, 18 and 20 are currently pending and have been examined fully.

Response to Arguments

5. Per claim 13, the Examiner due to Applicants argument has withdrawn the Claim rejection of 35 U.S.C. 112, second paragraph.

6. Applicant's arguments regarding independent claims 6, 12, 14, 16, 18 and 20 have been fully considered but they are not persuasive. The Applicant has argued that Downs fails to disclose (or suggest) the step of generating, in response to an attach/detach key information generation request and attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key. As noted below, the Examiner feels Downs does teach these limitations. The Examiner has interpreted a request for content along with specific encryption keys (col. 7, lines 10-40) as the "attach/detach information generation request and attach/detach key-specific encryption key". Examiner has also interpreted the fact that in the Specification of Downs it is explained, "The encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in SCs (described below) by the SC Packer Tool and stored in a content hosting site and/or promotional web site for electronic distribution. The content hosting site can reside at the Content Provider(s) 101 or in multiple locations, including Electronic Digital Content Store(s) 103 and Intermediate Market Partners (not shown) facilities. Since both the Content 113 and the Keys (described below) are encrypted and packed in SCs, Electronic Digital Content Store(s) 103 or any other hosting agent can not directly access decrypted Content 113 without clearance from the Clearinghouse(s) and notification to the Content Provider(s) 101." (col. 9, lines 48-60), and therefore the Examiner has interpreted this to be the hardware key. Site connected to site are frequently disconnected from each other due to bad connections, etc, and therefore it is also attachable/detachable. As per the arguments

regarding 6, 12, 13, 14, 16, 18 and 20, they have been fully considered but are moot in view of the grounds of rejection. Per each of the above-mentioned claims, the Applicant argues Downs does not teach “a hardware key including attach/detach key information”. As mentioned in the last argument, the Examiner is interpreting the content of Downs’ specification (col. 9, lines 48-60) as pertaining to the “hardware key” that stores attach/detach key information and that is attachable/detachable to the processor.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 6-12 and 14, 16, 18 and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Downs et al. (U.S. Patent No. 6,226,618) [hereinafter Downs].

9. As per claim 6, Downs teaches a license issuance server for issuing a license for execution of software, comprising:

- **attach/detach key information issuing means, responsive to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, for generating attach/detach key information including the device identification information and an attach/detach key-specific encryption key** (Fig. 1A – element 152; col. 7, lines 11-40)**, and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (The encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in SCs (described below) by the SC Packer Tool and stored in a content hosting site and/or promotional web site for electronic distribution. The content hosting site can reside at the Content Provider(s) 101 or in multiple locations, including Electronic Digital Content Store(s) 103 and Intermediate Market Partners (not shown) facilities. Since both the Content 113 and the

Keys (described below) are encrypted and packed in SCs, Electronic Digital Content Store(s) 103 or any other hosting agent can not directly access decrypted Content 113 without clearance from the Clearinghouse(s) and notification to the Content Provider(s) 101." (col. 9, lines 48-60), A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47));

- **license issuing means, responsive to a license issue request for the software, for encrypting a software decryption key for decrypting the software which is provided in an encrypted state** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, (abstract)), **by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (and the encrypted data being accessible to the user's system (abstract; Examiner is interpreting the fact that the attach/detach mechanism can be used for the invention that any encryption key assigned to the device is specific to that device)).

10. As per claim 7, Downs teaches claim 6 as described above. Downs further teaches **wherein said license issuing means includes, in the license information, a license count indicating a number of devices permitted to simultaneously execute the software** (Usage

Conditions – A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User (s) for use of the Content (col. 29, lines 40-42)).

11. As per claim 8, Downs teaches claim 6 as described above. Downs further teaches **wherein said hardware key has tamper resistance** (The Secret User Key (not shown) is protected by breaking the key into multiple parts and storing pieces of the key in multiple locations throughout the End-User(s)' computer. This area of the code is protected with Tamper Resistant Software technology so as not to divulge how the key is segmented and where it is stored. Preventing access to this key by even the End-User(s) helps to prevent piracy or sharing of the Content 113 with other computers (col. 80, lines 30-38)).

12. As per claim 9, Downs teaches claim 6 as described above. Downs further teaches **wherein said license issuing means encrypts the license information before outputting same** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

13. As per claim 10, Downs teaches claim 9 as described above. Downs further teaches **wherein said license issuing means encrypts the license information by using the attach/detach key-specific encryption key** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

14. As per claim 11, Downs teaches claim 6 as described above. Downs further teaches **further comprising license issue charge calculating means for storing past records on the license information output from said license issuing means, and calculating, based on the stored license information, a license issue charge to be billed to a provider of the software** (The Clearinghouse Transaction Log 178 can be used by the Content Provider(s) 101 to determine what Content 113 of his has been sold and enables him to create a bill to each Electronic Digital Content Store(s) 103 for royalties owed him. Other electronic means besides billing can alternatively be used to settle accounts between the Content Provider(s) 101 and Electronic Digital Content Store(s) 103 (col. 76, lines 18-25)).

15. As per claim 12, Downs teaches a software provision server for providing software whose execution is to be restricted by a license, comprising:

- **attach/detach key information issuing means, responsive to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, for generating attach/detach key information including the device identification information and an attach/detach key-specific encryption key** (Fig. 1A), **and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3), A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47));

- **software encryption key generating means** (Step Process 301 Sender generates a random symmetric key and uses it to encrypt the content. 302 Sender runs the encrypted content through a hash algorithm to produce the content digest (Fig. 3, col. 15)) **for generating a software encryption key for encrypting and decrypting the software, and a software decryption key for decrypting data encrypted by using the software encryption key** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **software encrypting means for encrypting the software by using the software encryption key generated by said software encryption key generating means** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **software providing means, responsive to input of a software request from the processing device, for transmitting the software encrypted by said software encrypting means to the processing device** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));

- **license issuing means, responsive to a license issue request for the software, for encrypting the software decryption key by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key… and the encrypted data being accessible to the user's system (abstract; Examiner is interpreting the fact that the attach/detach mechanism can be used for the invention that any encryption key assigned to said device is specific to said device)).

16. As per claim 14, Downs teaches a software execution management device for managing status of execution of software whose execution is restricted by a license, comprising:

- **a recording medium on which device identification information is fixedly recorded** (Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from. This information may be used to combat illegal use of the Content (col. 7-8, lines 66-67 and 1-5));

- **hardware key connecting means for reading attach/detach key information including an attach/detach key-specific encryption key and permission target device identification information specifying a device which is a target of permission to run the software, from a hardware key storing the attach/detach key information when the hardware key is attached** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47), Another encrypted object, in this example a Transaction ID encrypted object 205 is shown. And Usage Conditions 206 for content licensing management as described below. The SC(s) 200 comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed with an End-User Digital Signature 202 (col. 14-15, lines 63-67 and 1-5));

- **software key decrypting means, responsive to input of license information including an encrypted software decryption key for decrypting the software which has been**

encrypted and a number of computers permitted to execute the software simultaneously, for decrypting the software decryption key by using the attach/detach key-specific encryption key (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract; Examiner is interpreting "a number of computers" as allowing one computer connected));

- **decryption key managing means for monitoring computers connected via a network to detect a number of computers executing the software, and transferring the software decryption key decrypted by said software key decrypting means to a number of computers equal to or smaller than the number of computers permitted to execute the software simultaneously** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract); The Content Dispersement Tool provides a user the ability to implement the Content Dispersement Process 814 as described above. Once the Content 113 has been approved for release, the SC(s) for the Content 113 are placed in the queue of the Content Dispersement Process. The Content Dispersement Tool monitors the queue and performs immediate transfer of the SC(s) files or batch transfer of a group of SC(s) files based on the configuration settings provided by the Content Provider(s) 101. The Content Provider(s) 101 can also optionally configure the Content Dispersement Tool to automatically hold all SC(s) in this queue until they are manually flagged for release (col. 67, lines 35-46)).

17. As per claim 16, Downs teaches a license issuing method for issuing a license for execution of software, comprising the steps of:

- **generating, in response to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, attach/detach key information including the device identification information and an attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software decryption key for decrypting the software provided in an encrypted state, by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (When the End- User(s) completes shopping they submit the purchase request to the Electronic digital Content Store(s) 103 for processing (col. 18); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

18. As per claim 18, Downs teaches a license issuing program for issuing a license for execution of software, wherein said license issuing program causes a computer to perform the processes of:

- **generating, in response to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, attach/detach key information including the device identification information and an attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key which can be attached to and detached from the processing device** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software decryption key for decrypting the software provided in an encrypted state, by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (When the End- User(s) completes shopping they submit the purchase request to the Electronic digital Content Store(s) 103 for processing (col. 18); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

19. As per claim 20, Downs teaches a computer-readable recording medium recording a license issuing program for issuing a license for execution of software, wherein the license issuing program causes the computer to perform the processes of:

- **generating, in response to an attach/detach key information generation request including device identification information fixedly recorded on a recording medium in a processing device which is a target of permission to run the software, attach/detach key information including the device identification information and an attach/detach key-specific encryption key, and recording the generated attach/detach key information on a hardware key which can be attached to and**

detached from the processing device (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 5, The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement (col. 27, lines 15-17));

- **encrypting, in response to a license issue request for the software, a software decryption key for decrypting the software provided in an encrypted state, by using the attach/detach key-specific encryption key, and outputting license information including the encrypted software decryption key** (When the End- User(s) completes shopping they submit the purchase request to the Electronic digital Content Store(s) 103 for processing (col. 18); Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Downs in view of Johnson et al. (U.S. Patent No. 5,859,935).

22. As per claim 13, Downs teaches a processing device for executing software whose execution is restricted by a license, comprising:

- **a recording medium on which device identification information is fixedly recorded** (Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from. This information may be used to combat illegal use of the Content (col. 7-8, lines 66-67 and 1-5));

- **hardware key connecting means for reading attach/detach key information** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3)) **including an attach/detach key-specific encryption key and permission**

target device identification information specifying a device which is a target of permission to run the software, from a hardware key storing the attach/detach key information when the hardware key is attached (A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance (col. 9, lines 18-21). These can be adapted to follow technical advances in digital content compression/encoding, encryption, and formatting methods, allowing the Content Provider(s) 101 to utilize best tools as they evolve over time in the marketplace (col. 9, lines 43-47));

- **software key decrypting means, responsive to input of license information including an encrypted software decryption key for decrypting the software which has been encrypted, for decrypting the software decryption key by using the attach/detach key-specific encryption key** (Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract));
- **identification information determining means for determining sameness of the permission target device identification information included in the hardware key attached to said hardware key connecting means with the device identification information recorded on said recording medium** (It should be understood that this process like any of the other processes described on the Work Flow Manager 154 can run on a variety of hardware and software platforms. This method may be practiced on any

computer readable medium, including but not limited to floppy diskettes, CD ROMS and removable hard disk drives (col. 53-54 and lines 65-67 and 1-3); Fig. 2, The SC(s) 200 comprises Usage Conditions 206, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed with an End-User Digital Signature 202 (col. 15, lines 1-5));

- ***software decrypting means for decrypting the encrypted software by using the software decryption key decrypted by said software key decrypting means if the sameness is confirmed by said identification information determining means*** *(Disclosed is a method and apparatus of securely providing data to a user's system. The data is encrypted so as to only be decryptable by a data decrypting key, the data decrypting key being encrypted using a first public key, and the encrypted data being accessible to the user's system (abstract)).*

However, Downs does not further teach the determination of sameness briefly described in the claim. Also, Downs does not teach wherein if the determination does come out equivalent, then the software gets sent to the issuer.

Johnson does teach the determination of sameness (Original source verifying data defining a first source verifying image are stored in memory. The first source verifying image can be produced by a human making marks by hand in a field of a form, which can then be provided by a scanner or a facsimile transmission through image input circuitry. If a second source verifying image is received that is the same as the first source verifying image, an operation is performed *that would not be performed if the images were not the same, such as an operation accessing a related item of data (abstract); A "sameness criterion" is a criterion that can be applied to an item of data indicating a measure of similarity between two images to obtain an item of data indicating whether the two images are the same (col. 8, lines 5-12)).*

Johnson also teaches wherein this verification of sameness must be performed before the action of transferring data can take place (For example, the first source verifying image can be received with a document image, and data defining the document image and the original source verifying data can be stored so that a source verifying image that is the same as the first source verifying image must be received before an operation can access the document data and provide it to image output circuitry for printing or facsimile transmission (abstract)).

Therefore, it would have been prima facie obvious to one of ordinary skill in the art at the time of the invention to incorporate the determination of sameness with Downs, for the useful purpose of indicating a minimum or maximum value of the measure of similarity that satisfies the criterion, or a range within which or outside which the measure of similarity satisfies the criterion, as taught by Johnson (col. 8, lines 8-12).

Claim Interpretations

23. Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing responses, to fully consider the reference in its entirety as potentially teaching all of part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

24. In light of Applicants' choice to pursue product claims, Applicants are also reminded that functional recitations using the word "for," "configured to," or other functional terms *(e.g.* see claim 16 which recites "for generating attach/detach key information" or "for decrypting the software which") have been considered but are given little patentable weight[1] because they fail to add any structural limitations and are thereby regarded as intended use language. To be especially clear, all limitations have been considered. However a recitation of the intended use in a product claim must result in a structural difference between the claimed product and the prior art in order to patentably distinguish the claimed product from the prior art. If the prior art structure is capable of performing the intended use, then it reads on the claimed limitation. *In re Casey*, 370 F.2d 576, 152 USPQ 235 (CCPA 1967) ("The manner or method in which such machine is to be utilized is not germane to the issue of patentability of the machine itself."); *In re Otto*, 136 USPQ 458, 459 (CCPA 1963). See also MPEP §§ 2114 and 2115. Unless expressly

[1] See e.g. *In re Gulack*, 703 F.2d 1381, 217 USPQ 401, 404 (Fed. Cir. 1983)(stating that although all limitations must be considered, not all limitations are entitled to patentable weight.).

noted otherwise by the Examiner, the claim interpretation principles in this paragraph apply to all examined claims currently pending.

Conclusion

25. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

06/13/2007

Peter L. Ludwig
Patent Examiner
Art Unit 3621

AFischer 6/18/07

ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600